Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Secure Mobile Support of Independent Sales Agencies

Jochen Kokemueller
Fraunhofer Institute, jochen@kokemueller.de

Heiko Rossnagel
Fraunhofer Institute, heiko.rossnagel@iao.fraunhofer.de

Anette Weisbecker
Fraunhofer Institute, anette.weisbecker@aio.fraunhofer.de

Secure Mobile Support of Independent Sales Agencies

Jochen Kokemüller
Fraunhofer-Institute for Industrial Engineering
Jochen.Kokemueller@iao.fraunhofer.de

Heiko Roßnagel
Fraunhofer-Institute for Industrial Engineering
Heiko.Rossnagel@iao.fraunhofer.de

Anette Weisbecker
Fraunhofer-Institute for Industrial Engineering
Anette.Weisbecker@iao.fraunhofer.de

ABSTRACT

Sales agents depend on mobile support systems for their daily work. Independent sales agencies, however, are not able to facilitate this kind of mobile support on their own due to their small size and lack of the necessary funds. Since their processes correlate with confidential information and include the initiation and alteration of legally binding transactions they have a high need for security. In this contribution we first propose an IT-artifact consisting of a service platform that supports multi-vendor sales processes based on previous work. We then analyze use cases of sales representatives of independent sales agencies using this system and derive their security requirements. We then propose a security extension to the IT-artifact and evaluate this extension by comparing it to existing solutions. Our results show that the proposed artifact extension provides a more convenient and secure solution than already existing approaches.

Keywords

independent sales agencies, mobile services, security, design science.

INTRODUCTION

Sales agents depend on mobile support systems for their daily work. In the food industry for example sales agents use highly integrated mobile devices that allow order processing and barcode scanning to improve the productivity significantly (Walker and Barnes 2005). Usually these systems are connected to a customer relationship management (CRM) or enterprise resource planning (ERP) system at the vendor's site. Solutions that support the mobile workforce with online access to the corporate network typically require sophisticated techniques and mechanisms, as business transactions have inherently strong requirements with respect to security (Haller, Robinson, Walter and Kilian-Kehr 2002). Large companies with central IT management and a strategic commitment are able to facilitate this kind of mobile support. Due to their size and their common processes, these companies can choose from a broad range of systems to support them (Benz, Ritz and Stender 2003). In addition they can undertake the necessary steps to build a proper infrastructure for authentication and access management and secure the mobile access to their backend (Karjoth 2003).

Independent sales agencies (ISA), on the other hand, are not able to facilitate this kind of mobile support on their own. According to (Kokemüller, Kett, Höß and Weisbecker 2008) these agencies have an average of 4.1 employees not counting the owners of the agency. Additionally, 96% have no more than 5 field workers with the average being 1.7. Therefore, most independent commercial agencies clearly qualify as micro-sized enterprises. Due to their small size and lack of the necessary funds they are not able to build and maintain the required infrastructure (Kokemüller et al. 2008). Yet ISAs would largely benefit from mobile support such as mobile access to last minute information, the ability to perform documentation duties and transactional access to distributed backend systems. Furthermore, 93% of those agencies operate for more then one supplier (Kokemüller et al. 2008) causing the need to support multi-vendor sales processes. Therefore, there should be a demand for a system that supports multi-vendor sales processes, provide the necessary amount of security and is yet affordable to small size enterprises. Due to the integration of multiple legacy systems of different vendors such a mobile support system has to address a highly heterogeneous environment while still being reasonable economic. To our knowledge solutions that satisfy these needs are currently not available on the market. Therefore, systems that solve the problems of typical small ISAs still bear large opportunities both in research and on the market. In this contribution we analyze the security requirements of such a system and discuss possible implementations to fulfill them.

The rest of the paper is structured as follows. We begin with an outline of our methodological approach. We then present a detailed description of the application scenario for a mobile support system. We continue with a use case analysis for sales representatives of independent sales agencies. Based on these use cases we derive security requirements of this system. We propose an extension to the mobile support system to fulfill these security requirements and evaluate it against other already existing approaches before we summarize our results.

METHODOLOGICAL APPROACH

Design science research contributions present novel IT-artifacts and suitable evaluation approaches that address the artifact's appropriateness to contribute to the problems' solution (Nunamaker, Chen and Purdin 1991). These two facets of rigorous design science-oriented research contribute to the foundations and the methodologies pool of Information Systems research, i.e. they contribute to its knowledge base (Hevner, March, Park and Ram 2004). In our work we follow this research paradigm. We first addressed the introduced problem (mobile support for independent sales agencies) with a system design providing a technological basis for mobile support of multi-vendor sales processes. This system represents an IT artifact instantiation that aims at contributing to the problem's solution, demonstrates the feasibility of the approach and has been presented in (Kokemüller et al. 2008).

In this contribution we take a close look at the mobile support component and its security requirements. We start by providing an extensive description of the problem domain by conducting a use case analysis for sales representatives of independent sales agencies. We then derive security requirements based on these use cases. We address these requirements by proposing a security extension to the IT-artifact, which forms a new IT-artifact itself. This new IT-artifact is evaluated by comparing it to already existing solutions. This evaluation is provided in form of an informed argument based on the derived security requirements, which is according to (Hevner et al. 2004) a suitable descriptive method for the evaluation of an IT-artifact. Therefore, we follow the classic approach of design science-oriented research as we first developed an IT artifact and we second provide an evaluation of the artifact.

SYSTEM OVERVIEW

Independent sales agencies are companies that represent one or more vendors. Their employees are sales representatives who offer the vendor's products to the customers. These products vary from standard products that can be ordered from a catalog to highly individualized products manufactured to the specific needs of a customer (Dolmetsch 2000). Independent sales agencies can be categorized in two dimensions. One dimension is their territorial exclusivity or lack of it. Sales agencies that have territorial exclusivity are the only representation of a specific vendor in a particular territory. They may still represent more than one vendor in that territory if the products are not competitive but no other sales agency is permitted to represent the vendor in that territory. ISAs without territorial protection still possess customer protection. Therefore, they receive a commission if they provide at least a minor contribution to a transaction leading to a payment. The second dimension is the power of contract. ISAs who possess this power are able to act in the name of the vendor and to execute a declaration of its intention. These are legally binding to the vendor. Both of the discussed dimensions can have different values for a particular ISA, depending on each vendor the ISA represents. Independent sales agencies generate revenue by receiving commissions for each transaction of the corresponding vendor that is legally connected to a payment. For ISAs with territorial exclusivity all revenue created in the granted territory yield to accrued commission

The project M3V (www.m3v-projekt.de) which is funded by the Federal German Ministry of Economy and Technology focuses on the design and development of a mobile multi-supplier sales information platform which electronically supports the sales processes between ISAs, their suppliers and their customers. This mobile support system is hosted by a service provider, who integrates the legacy systems of the vendors (Kokemüller et al. 2008). Figure 1 gives an overview of this scenario.

COLLABORATIVE MULTI-VENDOR SALES PROCESSES

Starting from the known processes we derived the central use cases the platform has to fulfill. In the following we present a short overview of these use cases. A more detailed description of the processes and use cases can be found in (Kett, Kokemüller, Höß, Engelbach and Weisbecker 2008).

Use Case 1: Management of customer data. The sales representatives should be able to manage the data of the customers. This data comprises of address data of the customer, the data of the contact persons and possibly personal remarks of the sales agent. While the personal remarks should only be accessible for the particular sales agent who wrote them, the address data should be readable for all members of the sales agency.

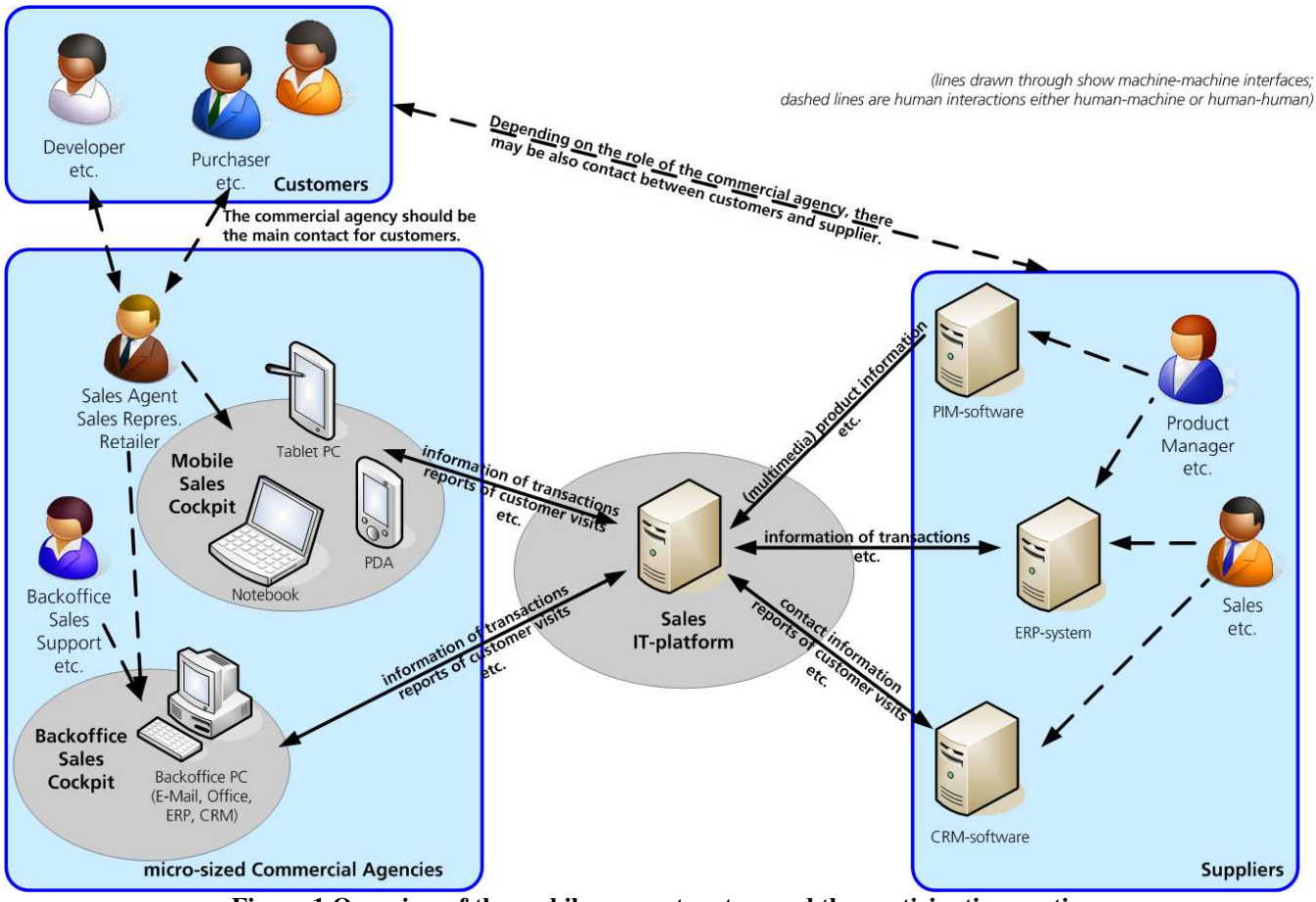

Figure 1 Overview of the mobile support system and the participating parties

Use Case 2: Visit reports. To ensure the vendor that it provides a complete and thorough coverage of the assigned territory the sales agency produces a report after each visit to a customer. In this report the sales agency provides information about the topics tackled, possible leads that should be followed in the future and general information about the customer. These visit reports are important in the case of ISAs without territorial exclusivity, because all revenues generated where an involvement of this ISA can be documented yield to accrued commission for the ISA. Additionally visit reports are important in the case of ISAs with territorial exclusivity, to demonstrate their activity in the granted territory.

Use Case 3: Recall of the customer's history. For the preparation of a visit a sales representative should be able to check the history of the customer. This includes prior visit reports, to refresh the information on potential leads to pursue during the sales visit. The knowledge of current transactions such as outstanding payments or expected deliveries can also be very beneficial.

Use Case 4: Access to catalog data. Especially standard products can be held in catalogs. Vendors often grant different sales privileges on their products to different ISAs. The catalogs may differ in the assortment, the prices or the bargain limits. Therefore, the catalog of a specific ISA in the platform is unique and not shared between ISAs representing the same vendor. From the catalog the ISA creates a request for quotation. This might include unstructured data to request a quote that exceeds the privileges granted.

Use Case 5: Unstructured requests for quotation. ISAs are often not able to provide a concise request for quotation. This is especially the case in regard to highly complex products, which might be specifically tailored for each customer. In order to create the request for quotation, the ISA composes an unstructured document describing the needs of the customer, requesting that the vendor might provide an elaborate quote.

Use Case 6: Creation of quotes. If a vendor has assigned power of contract to an ISA the sales representative can provide quotes to the customer, which when accepted will result directly in an order. As a consequence the details of the order are legally binding to the vendor.

SECURITY REQUIREMENTS

Having identified the relevant use cases for the presented scenario, we are now able to analyze their security requirements. For our analysis we used the confidentiality, integrity, and availability (CIA) triangle that forms the fundamental basis of IT security (Swanson 2001; Kesh and Ratnasingam 2007). We also added the security goal of accountability (Pfitzmann 2006) to our analysis. As the platform is used to perform transactions on sensible business data, confidentiality of the data transferred should be preserved at all times (Ghosh and Swaminatha 2001). Therefore, we can formulate a first general security requirement for the platform:

Requirement 1: The confidentiality of transferred data should be preserved at all times.

Since the mobile sales representatives are located outside the security domain of the service provider it is very important to make sure that access to this information service is appropriately secured (Schulz 2007). Therefore, access to the information service should only be granted to clients that have been securely identified and authenticated (Clarke and Furnell 2007). This leads to a second general security requirement.

Requirement 2: Access to the service platform should only be granted to clients that have been securely identified and authenticated.

We will now further elaborate the additional security requirements for each use case defined above.

Management of customer data:

Since customer data is a vital asset of any sales agency, it is important that updates of the customer data are performed exactly as they are entered by the sales representatives using their mobile devices. Therefore, we can formulate a requirement for the management of customer data.

Requirement 3: The service platform should provide means to detect violations of the integrity of transferred customer data.

The availability of the service platform is not critical for this particular use case. It can be addressed sufficiently by synchronizing the data later on. Using synchronization might reduce the service quality, because updates are held back, until the sales representative has a connection to the platform. This could even lead to a possible delay of several hours before an update is performed. However, this is only a concern if another person needs to access this data in the meantime. As the sales representative is the main contact person of the vendor at the customer's site, this is possible but not very likely. Also the accountability of the performed transactions is, apart from the proper authentication addressed by Requirement 2, not mission critical for this use case.

Visit reports:

Visit reports are important documents to both, the vendor and the sales representative. They provide information on upcoming sales opportunities and document the customer's situation. Often quotes are generated based on the information that was initially part of a visit report. If this information is altered during the transmission from the sales representative to the service platform, this could lead to monetary losses of vendors or the sales agency due to missed business opportunities. As a consequence any violations of the integrity of these reports must be recognized by the service platform.

Requirement 4: The service platform should provide means to detect any violations of the integrity of visit reports.

Similarly, as visit reports can be documents that prove the involvement of a sales representative in a sales activity that leads to accrued commission, accountability of these reports is of major importance even beyond the proper authentication addressed in Requirement 2. Several levels of accountability are possible. First of all non-repudiation of the visit report should be provided by the service platform. This leads to another requirement.

Requirement 5: The service platform should provide means to ensure that the origin of the visit reports can not be reputed.

In addition, a trustworthy documentation of the date and time the visit report was generated is desirable. This could be provided by the service platform. Optionally a proof of the location where the visit report was generated could also be offered by the service platform. Similar to the management of customer data use case, seamless availability of the service platform is not of major importance. A time spread between the generation of the visit report and its delivery reduces the service quality but does not circumvent the use case. However, if a trustworthy documentation of the time of the visit report generation is

performed it will register the time of the synchronization and not necessarily the time of the actual generation. This should not pose a significant problem, since the documentation of these reports is rather a matter of dates than of actual time.

Recall of the customer's history:

The access to the customer's history is crucial to the sales representative in the preparation of a visit. Naturally, the integrity of the accessed data is of major importance. Therefore, the service platform should provide means to detect violations of the integrity of the data, which leads to another requirement.

Requirement 6: *The service platform should provide means to detect any violations of the integrity of the customer's history.*

Apart from the proper authentication addressed in Requirement 2 no further form of accountability is required for this use case. Obviously, availability of the customer history is a prerequisite for this particular use case. The sales representative needs this information when requesting it, whether it is in the back-office or at the parking lot at the customer's location. The lack of this information circumvents this use case. Therefore, the service platform should provide means to ensure that the customer data is available to the sales representative.

Requirement 7: *The service platform should provide means to ensure that the customer data and history is available to the sales representative.*

Furthermore, since updates to the customer history could occur while the sales representative is already on the road, the service platform should undertake steps to keep the data as up-to-date as possible.

Access to catalog data:

This use case has similar security requirements as the recall of the customer data and history. It is important that changes to the data during transmission can be detected and therefore the service platform should provide the necessary means for it.

Requirement 8: *The service platform should provide means to detect any violations of the integrity of the catalog data.*

Also no form of accountability beyond the proper authentication is mandatory. The availability of the service platform that is required by this use case is dependent on the frequency of catalog changes. If the catalog data remains rather static, synchronization at the office should be sufficient. A high volatility of the catalog data, however, would require periodic updates and therefore a high degree of availability. This leads to a conditional requirement.

Requirement 9: *In case of a high volatility of the catalog data the service platform has to ensure the availability of up-to-date catalog data.*

Unstructured requests for quotation:

The security requirements of this use case are similar to those of the generation of visit reports. The sales agent composes an unstructured document describing the needs of the customer, requesting that the vendor might provide an elaborate quote. Obviously changes to the content of the request could have significant negative implications. Therefore, alterations during transmissions have to be detected.

Requirement 10: *The service platform should provide means to detect any violations of the integrity of requests for quotation.*

Furthermore, as requests for quotations are clearly documenting sales activity that influences commissions, accountability of these requests is of major importance and the service platform should document them. The service platform should document the content and time of the request in a way that can not be repudiated and provides a reliable proof of the sales representative's activity. The availability of the service platform is not crucial; as a time delay of a few hours does not circumvent the use case. Nevertheless it certainly lowers its service quality.

Creation of quotes:

If a vendor has assigned power of contract to an ISA, the sales representative can create a legally binding contract with the customer. Naturally, integrity and accountability of such a contract are necessities. Therefore, the service platform should provide means to detect violations of the integrity of created quotes.

Requirement 11: *The service platform should provide means to detect any violations of the integrity of created quotes.*

Also, non-repudiation of the quotes should be provided by the service platform. Furthermore, documentation of the time the quote was authored is essential, to prove the involvement of the ISA prior to the transaction. This leads to another requirement.

Requirement 12: *The service platform should provide means to ensure that the origin and time of the quotes can not be reputed.*

The required availability of the service platform is dependent on the degree of service integration and time criticalness of the particular case. If the contract includes commitments that are based on time critical information, then the ordering process is usually time critical as well. Delivery dates are for examples based on production capacities or stockings. In this cases race conditions have to be avoided.

Requirement 13: *In the case of time critical information, the platform must ensure that transactions will only be started if they can be committed immediately to the backend systems.*

SECURITY EXTENSION OF THE IT-ARTIFACT

In order to fulfill the requirements we are now proposing a security extension to the IT-artifact. Parts of this proposal consist of traditional security measures that are prevalent on the market and widely used for similar systems. Where these measures provide acceptable security we encourage the continuance of their usage. For example Requirement 1 can easily be met by using Secure Socket Layer (SSL) or Transport Layer Security (TLS). On top of these traditional methods we propose the usage of SIM[1] cards that are capable of creating electronic signatures. The technology for such SIM cards exists but has not gained much market penetration so far. For example the WiTness project (Project Wireless Trust for Mobile Business 2002) sponsored by the European Union has developed such a SIM card that is capable of reating RSA signatures (Rivest, Shamir and Adleman 1978). Figure 2 gives an overview over the architecture of such a SIM card. These SIM cards could be used to provide a reliable authentication method (Requirement 2) and a suitable solution for the requirements regarding integrity and non-repudiation (3, 4, 5, 6, 8, 10, 11, 12).

The availability Requirement VII could be fulfilled by storing the data on the client device and using periodic synchronization updates. This would ensure that the data is up-to-date if the mobile device is able to connect to the service platform and at the same time ensure that the sales representative can recall recent customer data even in areas without a mobile connection. For the Requirements 9 and 13 synchronization is unsuitable. On the contrary, the service platform should only allow transactions to be performed if it can ensure that they are committed to the backend systems immediately in order to avoid race conditions. Table 1 provides an overview of the used methods and technologies and their fulfillment of the security requirements.

	Security Technology		
Security Goal	SSL / TLS	Electronic Signatures	Synchronization
Accountability		2[2],5, 8, 12	
Availability			7
Confidentiality	1		
Integrity		3, 4, 6, 8, 10, 11	

Table 1: Overview of the used security methods and technologies and their fulfillment of the security requirements

[1] Subscriber Identity Module

[2] The SSCD can be used as an authentication token

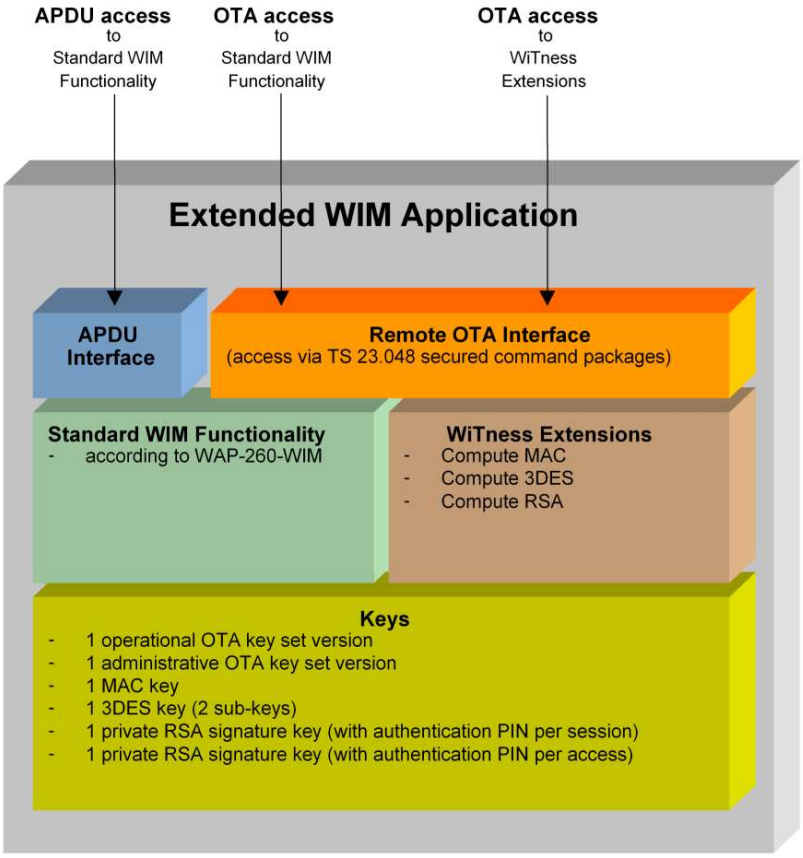

Figure 2: Overview of the architecture of the WiTness Prototype SIM card

EVALUATION

To evaluate our proposed security extension, we now compare our proposal against alternative solutions.

To achieve Requirement 2 one or more of three fundamental approaches could be used (Mayes and Piper 2005): something the user knows (password), something the user has (token) and something the user is (biometric). Usually passwords or external security token are used to allow this functionality (Karjoth 2003; Clarke and Furnell 2007). However, users tend to either choose weak passwords (Yan, Blackwell, Anderson and Grant 2004; Brown and Callis 2004), or choose related passwords for several or even all accounts (Adams, Sasse and Lunt 1997), which makes the authentication system vulnerable to cross-service attacks (Ives, Walsh, and Schneider 2004). External token, on the other hand, are expensive and stored on extra hardware that has to be connected to the device, needs to be carried around and can easily be lost (Clarke and Furnell 2007). Also, these token are usually proprietary solutions, which are only of use for one particular service. The use of a two factor authentication with a service independent security module present on the client device in combination with an authentication secret or biometric identification seems preferable.

Electronic signatures are a suitable solution for the requirements regarding integrity and non-repudiation (3, 4, 5, 6, 8, 10, 11, 12). These signatures are ideally performed by the same security module. If advanced electronic signatures with qualified certificates are used for signing the transactions this would also lead to reliable forensic evidence, which will be treated like handwritten signatures in any European court (Dumortier, Kelm, Nilsson, Skouma and Van Eecke 2003).

There are several different ways to implement security modules. It could either be a software component running on the mobile phone, some external security token that can be connected to the mobile phone or as in our proposal the SIM-card that is already present in a mobile phone.

However, if the legal reliability of advanced electronic signatures is desired (i.e. for the creation of quotes, see Requirements 11, 12), a secure signature creation device (SSCD) is mandatory, eliminating the possibility of a software solution. In this case using a SIM-card as SSCD instead of an external hardware token seems to be the better solution from a usability perspective (Roßnagel 2004).

LIMITATIONS

Introducing new technologies to ensure the integrity and accountability of the data will also lead to switching costs (Farrell and Shapiro 1988; Anderson 2001) that have to be incurred by the sales agency and its employees. Exchanging the SIM cards will induce additional costs for the mobile operator. These costs can be directly charged to the sales agencies increasing their switching costs or have to be compensated by an increase in mobile communication traffic caused by the new applications. In (Roßnagel and Royer 2005) and more detailed in (Roßnagel 2009) the profitability of such an exchange has been researched. The authors conclude that - given a promising service use case – the investment into such a technology can be profitable for mobile operators.

Since several sales agencies and vendors, who might compete with each other, are using the mobile support system, a fine grained access control is necessary. This is especially important, because customers can have business contacts to several ISAs present in the system. However, this is beyond the scope of this paper. Instead we focused on the mobile services.

CONCLUSION

In this contribution we have presented a mobile support system for independent sales agencies that provides multi-vendor support. We further analyzed the security requirements of this system based on identified use cases for sales representatives. Based on these requirements we proposed a security extension using signature capable SIM cards. Since several of the use cases have direct financial implications, even going as far as legally binding contracts when quotes are created, a trustworthy documentation is important. In these cases the usage of advanced electronic signatures with qualified certificates would be beneficial. In order to achieve these signatures, a SSCD is necessary. From a usability perspective, using a SIM-card instead of an external hardware token seems to be a more convenient solution. Consequently, SIM-card based signatures would provide means to ensure accountability and integrity. Therefore, they offer usable yet secure measures.

REFERENCES

1. Adams, A., Sasse, M. A. and Lunt, P. (1997) Making Passwords Secure and Usable*, Proceedings of HCI on People and Computers XII*, August, Bristol, Springer, 1-19.
2. Anderson, R. (2001) Why Information Security is Hard: An Economic Perspective*, Applied Computer Security Applications Conference (ACSAC 01)*, Dezember, Las Vegas, Nevada.
3. Benz, A., Ritz, T. and Stender, M. (2003) Marktstudie mobile CRM-Systeme, Fraunhofer IRB Verlag, Stuttgart.
4. Brown, B. J. and Callis, K. (2004) Computer Password Choice and Personality Traits Among College Students, Southeast Missouri State University, Cape Girardeau, Missouri.
5. Clarke, N. L. and Furnell, S. M. (2007) Advanced user authentication for mobile devices*, Computers & Security*, 26, 2, 109-119.
6. Dolmetsch, R. (2000) eProcurement, Addison Wesley, Boston.
7. Dumortier, J., Kelm, S., Nilsson, H., Skouma, G. and Van Eecke, P. (2003) The Legal and Market Aspects of Electronic Signatures, Interdisciplinary centre for Law & Information Technology, Katholieke University Leuven, Leuven*, http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf*, Oktober.
8. Farrell, J. and Shapiro, C. (1988) Dynamic competition with switching costs*, RAND Journal of Economics*, 19, 1, 123-137.
9. Ghosh, A. K. and Swaminatha, T. M. (2001) Software Security and Privacy Risks in Mobile E-Commerce: Examining the risks in wireless computing that will likely influence the emerging m-commerce market*, Communications of the ACM*, 44, 2, 51-57.
10. Haller, J., Robinson, P., Walter, T. and Kilian-Kehr, R. (2002) Framework and architecture for secure mobile business applications, inD. Gritzalis, S. De Capitani di Vimercati, P. Samarati and S. K. Katsikas (Eds.)*, Security and Privacy in the Age of Uncertainty, Proceedings of the IFIP TC11 International Conference on Information Security (SEC2003)*, May 26-28, Athens, Greece, Kluwer, 413-416.

11. Hevner, A. R., March, S. T., Park, J. and Ram, S. (2004) Design Science in Information Systems Research, *MIS Quaterly*, 28, 1, 75-105.
12. Ives, B., Walsh, K. R. and Schneider, H. (2004) The Domino Effect of Password Reuse, *Communications of the ACM*, 47, 4, 75-78.
13. Karjoth, G. (2003) Access Control with IBM Tivoli Access Manager, *ACM Transactions on Information and System Security*, 6, 2, 232-257.
14. Kesh, S. and Ratnasingam, P. (2007) A Knowledge Architecture for IT Security, *Communications of the ACM*, 50, 7, 103-108.
15. Kett, H., Kokemüller, J., Höß, O., Engelbach, W., Weisbecker, A. (2008) A mobile multi-supplier sales information system for micro-sized commercial agencies, *Proceedings of the eChallenges Conference 2008*, Stockholm.
16. Kokemüller, J., Kett, H., Höß, O. and Weisbecker, A. (2008) A Mobile Support System for Collaborative Multi-Vendor Sales Processes, *Proceedings of the 14th Americas Conference on Information Systems (AMCIS)*, 14.-17. August, Toronto.
17. Mayes, K. M. K. and Piper, F. (2005) Smart Card based authentication: Any Future?, *Computers & Security*, 24, 188-191.
18. Nunamaker, F. J., Chen, M. and Purdin, T. D. M. (1991) Systems development in information systems research, *Journal of Management Information Systems*, 7, 3, 89-106.
19. Pfitzmann, A. (2006) Multilateral Security: Enabling Technologies and Their Evaluation, in G. Müller (Eds.), *Emerging Trends in Information and Communication Security (ETRICS 2006), June 2006, Freiburg*, Springer, Heidelberg, 1-13.
20. Project Wireless Trust for Mobile Business (2002) Deliverable D4: SIM Application Hosting: Detailed Description of the Concept, Munich, Germany.
21. Rivest, R. L., Shamir, A. and Adleman, L. (1978) A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM*, 21, 2, 120-126.
22. Roßnagel, H. (2004) Mobile Signatures and Certification on Demand, in S. K. Katsikas, S. Gritzalis and J. Lopez (Eds.), *Public Key Infrastructures*, Springer, Berlin Heidelberg, 274-286.
23. Roßnagel, H. (2009) Mobile Qualifizierte Elektronische Signaturen: Analyse der Hemmnisfaktoren und Gestaltungsvorschläge zur Einführung, Gabler, Wiesbaden.
24. Roßnagel, H. and Royer, D. (2005) Profitability of Mobile Qualified Electronic Signatures, *Proceedings of the 9th Pacific Asia Conference on Information Systems (PACIS 05)*, Juli, Bangkok, AIS, 1345-1355.
25. Schulz, E. (2007) Mobile Computing: The next Pandora's Box, *Computers & Security*, 26, 3, 187.
26. Swanson, M. (2001) Security Self Assessment Guide for Information Technology Systems: Special Publication 800-26, National Institute for Standards and Technology, U.S. Government Printing Office, Washington, DC.
27. Walker, B. and Barnes, S. J. (2005) Wireless sales force automation: concept and cases, *International Journal of Mobile Communications*, 3, 4, 411-427.
28. Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2004) Password Memorability and Security: Empirical Results, *IEEE Security Privacy*, 2, 5, 25-31.